

Amendments to the Claims:

Please amend the Claims 1, 4, 10, 13, 18, and 21, and cancel Claim 20 without prejudice, and add new Claim 22, as follows.

Claim 1 (Currently Amended): A secure access card comprising:

at least one tone generator for generating tone audio output external from one side of the secure access card, the tone audio output comprising at least one tone signal that is variable in at least one of tone frequency, time duration of tone, time duration of space between tones, and by amplitude of tone, and wherein the at least one tone generator comprises a plurality of acoustic transducers that are mechanically tuned to oscillate about their mechanical resonant frequency to substantially maximize audio power output from each of the plurality of acoustic transducers being oriented outward of the one side of the secure access card for generating, from each of the plurality of acoustic transducers, the tone audio output external to the one side of the secure access card;

input means for accepting input from a user; and

a controller, electrically coupled to the at least one tone generator and the input means, for controlling the at least one tone generator to generate a tone sequence corresponding to the input from the user, the tone sequence for delivery via a communication network interface, the secure access card being of size and form for convenient carrying and use by a user.

Claim 2 (Original): The secure access card according to claim 1, wherein the at least one tone generator generates a tone sequence comprising at least one of dual tone multi-frequency (DTMF) signals, FSK signals, MSK signals, and multitone signals, to identify the user as an authorized user.

Claim 3 (Previously Presented): The secure access card according to claim 1, wherein the at least one tone generator further comprises a controllable amplifier circuit, the controller being electrically coupled to the controllable amplifier circuit and to the plurality of acoustic transducers to selectively control the controllable amplifier circuit and the plurality of acoustic transducers to generate the tone sequence corresponding to the input from the user.

Claim 4 (Currently Amended): The secure access card according to claim 1, wherein each of the plurality of acoustic transducers being oriented outward of the one side of the secure access card ~~for generating tone audio output external to one side of the secure access card and the plurality of acoustic transducers and further being located at the one side of the secure access card~~ for audio coupling the tone audio output from each of the plurality of acoustic transducers directed outward and external to the one side of the secure access card and to a telephone audio receiver for delivering a tone sequence via a communication network interface comprising a telephone network interface for a publicly switched telephone network (PSTN).

Claim 5 (Original): The secure access card according to claim 1, further comprising a memory for storing identification information, and wherein the controller is electrically coupled to the memory and to the input means for monitoring the input means for user input and to determine whether the user input matches the stored identification information to permit the card to generate the tone sequence for delivery via the communication network interface.

Claim 6 (Original): The secure access card according to claim 5, wherein the input means comprises at least one of a key input, a voice audio input, a signature input, and a fingerprint input, to capture user input from a user of the secure access card, the user input being compared to the stored identification information to permit the card to generate the tone sequence for delivery via the communication network interface.

Claim 7 (Original): The secure access card according to claim 1, further comprising a memory for storing a representation of user input, and wherein the controller is electrically coupled to the memory and to the input means for monitoring the input means for user input and to store a representation of the user input in the memory, the controller controlling the at least one tone generator to generate a tone sequence corresponding to the stored representation of the user input, the tone sequence for delivery via a communication network interface to a secure access server to determine whether the user input identifies the user as an authorized user of secure access function of a system.

Claim 8 (Original): The secure access card according to claim 7, wherein the input means comprises at least one of a key input, a voice audio input, a signature input, and a fingerprint input, to capture user input from a user of the secure access card and to store a representation of the user input in the memory, the controller controlling the at least one tone generator to generate a tone sequence corresponding to the stored representation of the user input for delivery via a communication network interface to a secure access server to determine whether the user input identifies the user as an authorized user of secure access function of a system.

Claim 9 (Previously Presented): The secure access card according to claim 7, wherein the tone sequence comprises a representation of the captured at least one of a key input, a voice audio input, a signature input, and a fingerprint input from a user of the secure access card to identify the user thereof.

Claim 10 (Currently Amended): A communication system comprising:

a communication network;
a secure application/function server, electrically coupled to the communication network, for providing secured access functions to an authorized user across the communication network;

a secure access server, electrically coupled to the communication network, for determining whether a user across the communication network is an authorized user, the secure access server including:

a network interface for coupling communication signaling between the communication network and the secure access server;

a tone signal processor electrically coupled to the network interface for receiving and processing communication signaling from the communication network, the communication signaling comprising at least one tone signal in a tone sequence;

a database memory for storing authorized user identification information including for each authorized user at least one of a personal identification number (PIN), a voice identification information, a fingerprint identification information, and a signature identification information; and

a controller, electrically coupled to the tone signal processor and the database memory, for receiving communication signaling from the communication network, the communication signaling comprising at least one tone signal in a tone sequence representative of user identification information, and for comparing the user identification information to the stored authorized user identification information to determine whether the user identification information received from across the communication network corresponds to an authorized user for accessing secured access functions provided by the secure application/function server to an authorized user across the communication network; and

a secure access card, being of size and form for convenient carrying and use by a user, including:

at least one tone generator for generating tone audio output external from one side of the secure access card, the tone audio output comprising at least one tone signal that is variable in at least one of tone frequency, time duration of tone, time duration of space between tones, and by amplitude of tone, and wherein the at least one tone generator comprises a plurality of acoustic transducers that are mechanically tuned to oscillate about their mechanical resonant frequency to substantially maximize audio power output from each of the plurality of acoustic transducers being oriented outward of the one side of the secure access card for generating, from each of the plurality of acoustic transducers, the tone audio output external to the one side of the secure access card;

input means for accepting input from a user; and

a controller, electrically coupled to the at least one tone generator and the input means, for controlling the at least one tone generator to generate a tone sequence corresponding to the input from the user and providing user identification information, the tone sequence for delivery via the communication network to the secure access server to identify the user as an authorized user for accessing secured access functions provided by the secure application/function server to the authorized user across the communication network.

Claim 11 (Previously Presented): The communication system according to claim 10, wherein the at least one tone generator generates a tone sequence comprising dual tone multi-frequency (DTMF) signals to identify the user as an authorized user.

Claim 12 (Previously Presented): The communication system according to claim 10, wherein the at least one tone generator further comprises a controllable amplifier circuit, the controller being electrically coupled to the controllable amplifier circuit and to the plurality of acoustic transducers to selectively control the controllable amplifier circuit and the plurality of acoustic transducers to generate the tone sequence corresponding to the input from the user.

Claim 13 (Currently Amended): The communication system according to claim 10, wherein each of the plurality of acoustic transducers being oriented outward of the one side of the secure access card for generating tone audio output external to one side of the secure access card and the plurality of acoustic transducers and further being located at the one side of the secure access card for audio coupling the tone audio output from each of the plurality of acoustic transducers directed outward and external to the one side of the secure access card and to a telephone audio receiver for delivering a tone sequence via the communication network comprising a publicly switched telephone network (PSTN).

Claim 14 (Previously Presented): The communication system according to claim 10, further comprising a memory for storing identification information, and wherein the controller is electrically coupled to the memory and to the input means for monitoring the input means for user input and to determine whether the user input matches the stored identification information to permit the card to generate the tone sequence for delivery via the communication network interface.

Claim 15 (Previously Presented): The communication system according to claim 14, wherein the input means comprises at least one of a key input, a voice audio input, a signature input, and a fingerprint input, to capture user input from a user of the secure access card, the user input being compared to the stored identification information to permit the card to generate the tone sequence for delivery via the communication network interface.

Claim 16 (Previously Presented): The communication system according to claim 10, further comprising a memory for storing a representation of user input, and wherein the controller is electrically coupled to the memory and to the input means for monitoring the input means for user input and to store a representation of the user input in the memory, the controller controlling the at least one tone generator to generate a tone sequence corresponding to the stored representation of the user input, the tone sequence for delivery via the communication network to the secure access server to determine whether the user input identifies the user as an authorized user of secure access function of a system.

Claim 17 (Previously Presented): The communication system according to claim 16, wherein the input means comprises at least one of a key input, a voice audio input, a signature input, and a fingerprint input, to capture user input from a user of the secure access card and to store a representation of the user input in the memory, the controller controlling the at least one tone generator to generate a tone sequence corresponding to the stored representation of the user input for delivery via the communication network to the secure access server to determine whether the user input identifies the user as an authorized user.

Claim 18 (Currently Amended): A method for a communication system comprising the steps of:

capturing user input at a secure access device, the secure access device being of size and form for convenient carrying and use by a user;
storing a representation of the user input at the secure access device;
acoustically transmitting by at least one tone generator in the secure access device tone audio output external from one side of the secure access device, the tone audio output comprising a tone sequence, including a first tone and a second tone different from the first tone, destined for reception across a communication network, the tone sequence corresponding to the stored representation of the user input, wherein the at least one tone generator comprises a plurality of acoustic transducers that are mechanically tuned to oscillate about their mechanical resonant frequency to substantially maximize audio power output from each of the plurality of acoustic

transducers being oriented outward of the one side of the secure access device for generating, from a first one of the plurality of acoustic transducers the first tone and from a second one of the plurality of acoustic transducers the second tone, the tone audio output external to the one side of the secure access device;

receiving from across the communication network a representation of the transmitted tone sequence;

comparing the received representation of the transmitted tone sequence to pre-stored authorized user identification information; and

determining whether a match between the representation of the transmitted tone sequence and a pre-stored authorized user identification information identifies the user of the secure access device as an authorized user of the communication system.

Claim 19 (Previously Presented): The method of claim 18, wherein the step of capturing user input at a secure access device comprises the step of:

capturing at least one of a key input, a voice audio input, a signature input, and a fingerprint input, to capture user input from a user of the secure access device.

Claim 20 (Canceled)

Claim 21 (Currently Amended): A secure access device comprising:

at least one tone generator for generating tone audio output external from one side of the secure access device, the tone audio output comprising a tone sequence including a first tone and a second tone different from the first tone, at least one tone signal that is variable in at least one of tone frequency, time duration of tone, time duration of space between tones, and by amplitude of tone, and wherein the at least one tone generator comprises a plurality of acoustic transducers being mechanically tuned to oscillate substantially at their mechanical resonant frequency to substantially maximize audio power output from each of the plurality of acoustic transducers being oriented outward of the one side of the secure access device for generating from a first one of the plurality of acoustic transducers the first tone and from a second one of the plurality of acoustic transducers the second tone, the tone audio output external to the one side of the secure access device, and wherein the secure access device being in a credit card form factor for convenient carrying and use by a user;

input means for accepting input from a user; and

a controller, electrically coupled to the at least one tone generator and the input means, for controlling the at least one tone generator to generate a tone sequence corresponding to the input from the user, the tone sequence for delivery via a communication network interface.

Claim 22 (New): The secure access card according to claim 1, wherein the secure access card being in a credit card form factor for convenient carrying and use by a user.